Amendments to the claims:

1. (currently amended) Method of updating an authentication algorithm used by a device (CARD) to authenticate with a data processing device (SERV) wherein the device (CARD) ~~can store in~~ has a memory element ~~of said device (CARD) a first~~ for storing a subscriber identity (IMSI~~1~~) which is associated with ~~a first~~ an authentication algorithm ~~(Algo1)~~, comprising:

- a first preoperational preliminary step of storing an active first authentication algorithm (Algo1) in a non-volatile memory element of the device (CARD) associated with a first subscriber identity (IMSI1);
- a second preoperational preliminary step of storing ~~a~~ an inactive second ~~inactive~~ authentication algorithm (Algo2) in a non-volatile memory element of the device (CARD) associated with a second subscriber identity (IMSI2); and
- a step for switching from the first authentication algorithm (Algo1) to the second authentication algorithm (Algo2) including permanently deactivating the first authentication algorithm (Algo1) and ~~activate~~ activating the second authentication algorithm (Algo2) used by the device (CARD).

2. (Previously Presented) Method according to claim 1, wherein the switching step is carried out on the initiative of an entity (OP) external to said device.

3. (Previously Presented) Method according to claim 1 or 2, wherein, to perform the switching operation, the entity (OP) external to said device transmits a command (COM) remotely to said device (CARD) in order to switch from the first authentication algorithm (Algo1) to the second authentication algorithm (Algo2).

4. (Previously Presented) Method according to claim 1 or 2, wherein, to perform the switching operation, the entity external to said device downloads into the device a

program which can start up after a time delay and whose purpose is to switch from the first authentication algorithm (Algo1) to the second authentication algorithm (Algo2).

5. (Previously Presented) Method according to claim 1, wherein, during the pre-storage step, a second code IMS12, different from a code IMSI1 associated with the first algorithm, and associated with the algorithm AIgo2, is stored, and wherein after the step for switching accounts on said device (CARD), said device (CARD) transmits the code IMS12 to all or some of the data processing devices (SERV) whose algorithms need to be switched, said second code (IMSI2) associated with the second algorithm informing these data processing devices that the algorithms have been switched in order to synchronise the algorithm update.

6. (Previously Presented) Method according to claim 5, wherein on reception of the second code (IMSI2) associated with the second authentication algorithm (Algo2), said receiving device switches algorithm from the first authentication algorithm (Algo1) to the second authentication algorithm (Algo2).

7. (Previously Presented) Method according to claim 1, wherein after switching, the memory space storing the data associated with the deactivated account is reused.

8. (Currently Amended) Data processing device, in particular a smart card ~~which can store~~ having a memory element for storing a ~~first~~ subscriber identity (IMSI~~1~~) and ~~which is~~ associated with ~~a first~~ an authentication algorithm (Algo~~1~~), comprising:

- first non-volatile memory means storing an active first authentication algorithm (Algo1) associated with a first subscriber identity (IMSI1),
- second non-volatile memory means storing ~~a~~ an inactive second authentication algorithm (Algo2) associated with a second subscriber identity (IMSI2),

- a microcontroller programmed to carry out a step for switching from the first authentication algorithm (Algo1) to the second authentication algorithm (Algo2), which ~~can~~ when executed permanently ~~deactivate~~ deactivates the first authentication algorithm (Algo1) and ~~activate~~ activates the second authentication algorithm (Algo2).

9. (Cancelled)

10. (Cancelled)

11. (Currently Amended) A non-volatile computer storage media operable to store instructions for instructing a data processing device, in particular a smart card, to perform certain operations, the storage media comprising:

an active first authentication algorithm (Algo1) associated with a first subscriber identity (IMSI1) stored in the non-volatile storage media during a pre-operational preliminary phase;

~~a~~ an inactive second ~~inactive~~ authentication algorithm (Algo2) associated with a second subscriber identity (IMSI2) stored in the non-volatile storage media during a pre-operational preliminary phase; and

instructions to direct the data processing device(CARD) to execute a step for switching from ~~a~~ the first authentication algorithm (Algo1) to ~~a~~ the second authentication algorithm (Algo2), which ~~can~~ when executed permanently ~~deactivate~~ deactivates the first authentication algorithm (Algo1) associated with a first subscriber identity (IMSI1) and ~~activate~~ activates the second authentication algorithm.

12. (Previously Presented) The storage media according to claim 11, further comprising instructions to direct the data processing device to perform the step of switching from the first authentication algorithm to the second authentication algorithm, upon receiving from a transmitting device a code IMSI2 different from the code IMSI1 and therefore associated with the second authentication algorithm Algo2.

13. (new) The method of updating an authentication algorithm used by a device (CARD) to authenticate with a data processing device (SERV) of Claim 1, wherein at least one of the first preoperational preliminary step and the second preoperational preliminary step is performed during card personalization.

14. (new) The computer storage media of Claim 11, wherein at least one of the first and second authentication algorithms is stored in the storage media during card personalization.